APPOSITE TECHNOLOGIES

CASE STUDY

Validation of Firewall and IDS Performance

How a Leading Defense Innovator Uses Netropy CyberAttack to Evaluate Threat Detection and Network Performance Under Real-World Conditions

In an era where advanced threats evolve daily, validating the performance of network security devices like firewalls and intrusion detection systems (IDS) is critical. One major defense organization set out to create a high-fidelity test environment that could accurately simulate real-world network conditions and threat activity. The goal: to rigorously evaluate how well their security solutions could detect and stop malicious activity, flag anomalies, and maintain high performance for legitimate traffic even under extreme conditions.

By partnering with Apposite Technologies, the organization gained a powerful platform to emulate complex, mixed-traffic scenarios, benchmark device performance, and validate security effectiveness without risking disruption to their production systems.

"The modern approach to security testing that Netropy CyberAttack brings has allowed us to configure and run complex test scenarios much faster than we could with our previous test systems."

HIGHLIGHTS

- New users productive in 50% less time than legacy system
- 30% more variety of application and threat traffic to test IDS/ Firewall
- Cost of new Apposite test system less than annual maintenance of legacy system

The Challenge

Security teams often face a difficult balance: blocking malicious traffic while ensuring uninterrupted performance for critical applications. The organization needed to answer several key questions:

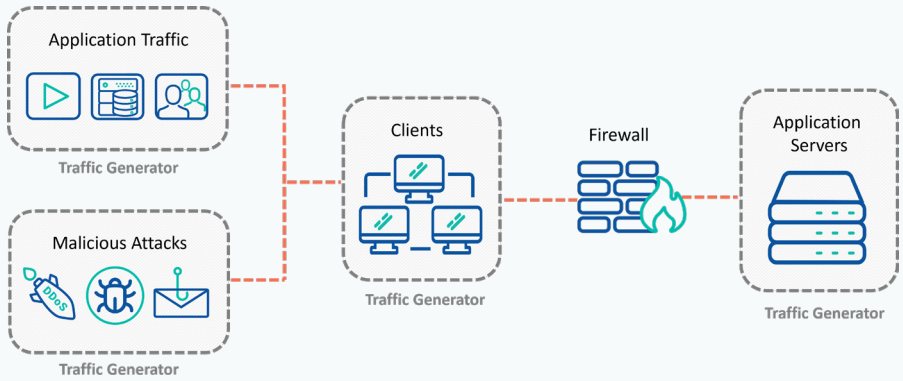
- *Can our IDS systems and firewalls detect and stop the latest threats?*
- *Will they allow mission-critical applications to function reliably under high traffic loads?*
- *How do these devices perform when faced with surges in traffic volume or session complexity?*
- *Can we evaluate these devices without causing outages or delays in a live environment?*

The solution had to be flexible, repeatable, easy to use, and able to simulate thousands of sessions and application types from routine enterprise traffic to cutting-edge cyberattacks.

The Approach

Apposite's high-scale threat emulation and application-aware traffic generation testing solution, Netropy CyberAttack, enabled the defense innovator to recreate real-world cyberattack scenarios with unmatched precision and control.

Security Device Test Diagram



Intrusion Detection System (IDS) Testing

To evaluate the effectiveness of their IDS, the team designed a comprehensive testing strategy that combined real-world traffic emulation with sophisticated threat simulations. Using Netropy CyberAttack they created diverse traffic patterns reflecting typical usage such as tactial communication applications, collaboration tools, encrypted video, and file transfers. Threat traffic was then incorporated to challenge the IDS across multiple dimensions:

- Signature-based threats, sourced from Apposite's up-to-date, CVE-aligned attack library
- Anomaly-based traffic, including subtle behavioral deviations that might indicate malware, misuse, or insider threats
- Encrypted attack payloads, to assess the IDS's ability to detect threats within secure channels
- Custom threat profiles, designed to emulate zero-day exploits and internal policy violations
- Noise injection and traffic variation, to evaluate false positive rates and the system's resilience under non-ideal conditions

By focusing on both signature recognition and anomaly detection, the team was able to measure the IDS's accuracy, responsiveness, and overall alerting effectiveness. This approach helped identify potential blind spots, tune system configurations, and confirm the IDS could reliably detect known threats while also adapting to new and evolving attack patterns that traditional tools might miss.

AI-Driven Threat Modeling

To keep pace with evolving threats, AI-based analytics were layered into the test approach. These capabilities helped uncover subtle behavioral anomalies, simulate evasive tactics, and validate the IDS's capacity to respond to previously unseen patterns. The fusion of AI modeling and high-scale traffic replay offered an even deeper insight into true threat readiness.

Firewall Performance Testing

The organization also needed to validate its firewall configurations to ensure they could enforce policy, block malicious traffic, and maintain performance under load. Using Apposite's high-scale traffic generation and up-to-date Attack Library, the team simulated:

- Legitimate traffic: Web, video, VoIP, file transfer, and other critical protocols
- Policy-violating traffic: Disallowed services like streaming media, gaming, or other restricted applications
- Malicious traffic: Realistic threats, including malware signatures, known CVEs, and behavior-based exploits from Apposite's continuously updated Attack Library

A key part of the evaluation involved testing the firewall's session handling capacity under stress, an often hidden limitation that can result in performance degradation. The team generated thousands of concurrent TCP sessionsand UDP flows to measure:

- Throughput and latency under high load
- Packet loss and connection stability as the volume scaled
- Session setup and teardown rates, identifying potential bottlenecks or slowdowns

With Apposite's granular control and repeatable testing, the organization fine-tuned both security and performance, ensuring their firewalls were ready for real-world demands.

Key Benefits and ROI

- **Validated Security Effectiveness:** Firewalls and IDS systems were strenuously evaluated on whether they could detect and mitigate high volumes of threat traffic while maintaining application throughput
- **Improved Accuracy and Resilience:** Tests revealed configuration gaps and tuning opportunities to be corrected before deployment
- **Increased Testing Agility:** New scenarios could be launched in minutes, with full automation for future regression testing
- **Improved Network Resilience:** Testing revealed bottlenecks in session handling and allowed for early optimization before deployment
- **Cost and Time Efficiency:** By testing in a simulated lab environment, the team avoided the cost and risk of production outages or service disruptions

The Results

Firewall and IDS systems are essential components of modern cybersecurity infrastructure, but assumptions about their performance can no longer go untested. Real-world validation is critical. This case shows how a defense innovator turned assumptions into evidence using Apposite's intuitive, scalable, and high-fidelity testing platform.

With Apposite, this defense organization gained full visibility into how their security devices behaved under pressure. They identified potential vulnerabilities, fine-tuned performance, and ensured their infrastructure was ready to defend against the threats of today and tomorrow.

Why Apposite

Apposite's cybersecurity testing platform offers the precision, speed, and usability required for today's high-stakes security environments:

- **Real-World Traffic Simulation**
  Simulate legitimate and malicious traffic simultaneously, including both signature-based and behavioral attack patterns
- **Custom Attack Profiles**
  Build complex threat scenarios using Apposite's continuously updated library of attacks to match evolving vulnerabilities or in-house risk models
- **Faster Time to Insight**
  Leverage RESTful API with Swagger support or Apposite's intuitive interface to build and repeat complex scenarios in minutes
- **Scalability and Flexibility**
  The same platform supports testing from 1Gbps portable environments to 100Gbps high-throughput deployments
- **Detailed Reporting**
  Real-time logs, intuitive graphs, and exportable formats allow teams to quickly analyze results and present findings

ABOUT APPOSITE

Apposite Technologies provides world-class network, application and security test solutions to enterprises, service providers, and government agencies worldwide. Offering both network emulation and traffic generation solutions, Apposite enables users to generate realistic application traffic and replicate accurate simulations of any wide-area network for a fast, easy way to optimize network and device performance.

Apposite's modern testing solutions help businesses deploy new technology with confidence while increasing automation and lowering costs associated with performance testing.

Apposite Technologies

4223 Glencoe Ave B121, Marina del Rey, CA 90292 USA

www.apposite-tech.com | TEL: 1.310.477.9955 | info@apposite-tech.com